



On (n, k) -sequences [☆]

Hong-Yeop Song^{a,*}, June Bok Lee^b

^aDepartment of Electrical and Computer Engineering, Yonsei University, Seoul 120-749, South Korea

^bDepartment of Mathematics, Yonsei University, Seoul 120-749, South Korea

Received 7 April 1999; revised 21 December 1999; accepted 22 December 1999

Abstract

An (n, k) -sequence has been studied. A permutation a_1, a_2, \dots, a_{kn} of $0, 1, \dots, kn - 1$ is an (n, k) -sequence if $a_{s+d} - a_s \not\equiv a_{t+d} - a_t \pmod{n}$ whenever $\lfloor a_{s+d}/n \rfloor = \lfloor a_s/n \rfloor$ and $\lfloor a_{t+d}/n \rfloor = \lfloor a_t/n \rfloor$ for every s, t and d with $1 \leq s < t < t + d \leq kn$, where $\lfloor x \rfloor$ is the integer part of x . We recall the “prime construction” of an (n, k) -sequence using a primitive root modulo p whenever $kn+1=p$ is an odd prime. In this paper we show that (n, k) -sequences from the prime construction for a given p are “essentially the same” with each other regardless of the choice of primitive roots modulo p . Further, we study some interesting properties of (n, k) -sequences, especially those from prime construction. Finally, we present an updated table of essentially distinct $(n, 2)$ -sequences for $n \leq 13$. The smallest n for which the existence of an $(n, 2)$ -sequences is open now becomes 16. © 2000 Elsevier Science B.V. All rights reserved.

Keywords: ; (n, k) -Sequences; Difference triangles; Singly periodic Costas sequences; Florentine and Vatican arrays; Frequency hopping codes

1. Introduction

Consider the sequence 0, 3, 4, 6, 7, 1, 5, 2 of length 8 (a_i for $1 \leq i \leq 8$) and its difference (mod 4) triangle in Fig. 1, where the difference $a_j - a_i \pmod{4}$ for $1 \leq i < j \leq 8$ is calculated whenever $a_i, a_j < 4$ or $a_i, a_j \geq 4$. We designate such a pair (a_i, a_j) as “comparable”. The asterisk * in the triangle represents an incomparable situation. Observe that in any row of this triangle the differences are all distinct modulo 4. We call this sequence a_1, a_2, \dots, a_8 a “(4, 2)-sequence”.

More generally, we can define “comparability” of a pair (a_i, a_j) to mean that the integer parts of both a_i/n and a_j/n are the same [10].

[☆] The authors wish to acknowledge the financial support of the Korea Research Foundation made in the program year of 1997.

* Corresponding author. Fax: +82 2 3124584.

E-mail addresses: hysong@yonsei.ac.kr (H.-Y. Song), leejb@yonsei.ac.kr (J.B. Lee).

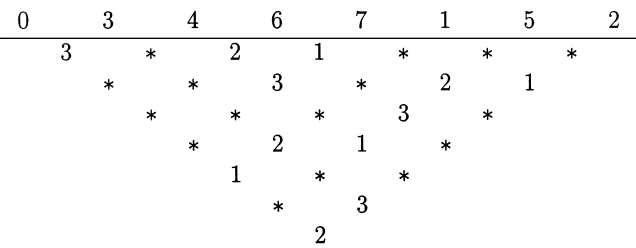


Fig. 1. Difference triangle (mod 4) of a (4,2)-sequence 0, 3, 4, 6, 7, 1, 5, 2.



Fig. 2. A 4×8 Vatican array having cyclic columns.

Definition 1. Let a_1, a_2, \dots, a_{kn} be a permutation of $0, 1, 2, \dots, kn - 1$. Let (a_i, a_j) be called a “comparable pair” if $\lfloor a_i/n \rfloor = \lfloor a_j/n \rfloor$, where $\lfloor x \rfloor$ is the integer part of x . Then, a_1, a_2, \dots, a_{kn} is called an “ (n, k) -sequence” if

$$a_{s+d} - a_s \not\equiv a_{t+d} - a_t \pmod n$$

whenever (a_s, a_{s+d}) and (a_t, a_{t+d}) are comparable pairs for every s, t and d with $1 \leq s < t < t + d \leq kn$.

From the (4,2)-sequence shown in Fig. 1, one can construct the following 4×8 array V of 8 symbols in which the top row is a_1, a_2, \dots, a_8 and the columns are cyclic shifts of either 0, 1, 2, 3 or 4, 5, 6, 7, as shown in Fig. 2. The array V has the two properties that (1) each row is a permutation of $0, 1, 2, \dots, 7$ and (2) for any two symbols a and b and for any integer m from 1 to 7 there exists at most one row in which b is m steps to the right of a . A $k \times n$ array which satisfies these properties is known as a “Florentine array” [4]. Further, the array V is actually a “Vatican array”, which is defined to be a Florentine array such that no two symbols are the same in any column [4].

The original motivation for (n, k) -sequences [10] was to construct Vatican arrays (and hence, Florentine arrays) of size $k \times nk$ as illustrated above, and this paper is to report any further results after [8,10,11].

Florentine and/or Vatican arrays (or squares) were extensively studied in [4,1,2,8, 13,9]. These combinatorial structures have a wide range of applications in communications engineering: design of frequency hopping patterns for multiple-access communications environments [5,9,12,13], design of radar and sonar arrays for improved

range-Doppler measurements [3], and design of modulation signals for optical PPM modulations [6]. They also find applications in the area of design of experiments [4,8] and in extremal graph theory such as edge-decompositions of complete directed graphs [1,2,14].

In [1,2], the polygonal-path construction for Florentine squares is introduced, in which the columns are cyclic shifts of each other. It was also proved that a polygonal-path Florentine square of size $n \times n$ exists if and only if there exists a “singly periodic Costas array” of size $n \times n$, or equivalently, a singly periodic Costas sequence of length n (which is an $(n, 1)$ -sequence in our terminology). Similarly, it was proved in [10] that if there exists an (n, k) -sequence of length kn then we can construct an $n \times kn$ Vatican array and hence an $n \times (kn + 1)$ Florentine array.

This paper is organized as follows. In Section 2, we recall the main construction [10] of (n, k) -sequences whenever $nk + 1 = p$ is an odd prime, and now prove that all such sequences of length nk are equivalent without regard to the choice of primitive roots mod p . In Section 3, we will investigate some further properties of (n, k) -sequences, especially, those from the “prime construction.” We were able to solve some of open problems posed in [10]. Finally, we present an updated table of $(n, 2)$ -sequences for $n \leq 13$ in Section 4.

2. Main construction and equivalence

Let $\{a_i \mid 1 \leq i \leq nk\}$ be an (n, k) -sequence. For each $j = 0, 1, \dots, k - 1$, let $S_j = \{a_i \mid nj \leq a_i \leq n(j + 1) - 1\}$. Then, S_j is a set of comparable pairs each other and a partition of the (n, k) -sequence. We will call S_j the j th comparable part of the (n, k) -sequence. For each $j = 0, 1, \dots, k - 1$ any member a_i of S_j can be written as $a_i = nj + t$; $t = 0, 1, \dots, n - 1$. Given an (n, k) -sequence $\{a_i \mid 1 \leq i \leq nk\}$ we can obtain another (n, k) -sequence $\{b_i \mid 1 \leq i \leq nk\}$ by the following transformations [10]:

- (A) For some S_j , b_i is obtained by adding some constant c to all the $a_i \in S_j$ so that $b_i = nj + d_i$ where $d_i \equiv a_i + c \pmod{n}$, $0 \leq d_i \leq n - 1$.
- (M) Let m be a constant which is relatively prime to n . For all S_j , b_i is obtained by multiplying m to all the $a_i \in S_j$ so that $b_i = nj + d_i$ where $d_i \equiv a_i m \pmod{n}$, $0 \leq d_i \leq n - 1$.
- (P) For each j, l with $0 \leq j < l \leq k - 1$ we replace $a_i = nj + d_i \in S_j$ by $b_i = nl + d_i \in S_l$ and replace $a_i = nl + d_i \in S_l$ by $b_i = nj + d_i \in S_j$.
- (R) b_i is obtained by the reverse order of a_i , namely $b_i = a_{nk-i+1}$ for all $i = 1, 2, \dots, nk$.

It is easy to check that $\{b_i \mid 1 \leq i \leq nk\}$ which is obtained by the above transformations is an (n, k) -sequence. We say that these two (n, k) -sequences $\{a_i\}$ and $\{b_i\}$ are “essentially the same”.

Theorem 2 (Main construction and equivalence). *Let g be a primitive root modulo $p = kn + 1 > 2$ where p is a prime. For $i = 1, 2, \dots, kn$, let $\text{Ind}_g i$ be the index of i with respect to g namely, $\text{Ind}_g i = j$ iff $i = g^j$ for some $j = 0, \dots, kn - 1$. Let q_i and*

r_i be integers such that $\text{Ind}_g i = kq_i + r_i$, where $0 \leq r_i \leq k-1$. Then, $a_i = q_i + nr_i$ for $i = 1, 2, \dots, kn$ is an (n, k) -sequence. Further, if h is another primitive root modulo p and $\{b_i\}$ is the (n, k) -sequence constructed likewise then, two (n, k) -sequences $\{a_i\}$ and $\{b_i\}$ are “essentially the same”.

Proof. See [10] for proof of the construction. Briefly, if (a_i, a_j) is a comparable pair then $r_i = \lfloor a_i/n \rfloor = \lfloor a_j/n \rfloor = r_j$ and thus $g^{ka_i}/g^{ka_j} \equiv i/j \pmod{p}$. Therefore, if $a_{s+d} - a_s \equiv a_{t+d} - a_t \pmod{n}$, we have $k(a_{s+d} - a_s) \equiv k(a_{t+d} - a_t) \pmod{kn}$, and hence we obtain $g^{k(a_{s+d}-a_s)} \equiv g^{k(a_{t+d}-a_t)} \pmod{p}$. This implies that $d \equiv 0$ or $s \equiv t \pmod{p}$.

Now, if h is another primitive root modulo p then, we have an (n, k) -sequence $\{b_i\}$ where $b_i = q'_i + nr'_i$ for which $\text{Ind}_h i = kq'_i + r'_i$ with $0 \leq r'_i \leq k-1$. Since h is a primitive root, $h = g^l$ for some l which is relatively prime to $p-1 = kn$ and $1 \leq l < kn$. Since $\text{Ind}_h i = \text{Ind}_{g^l} i = kq'_i + r'_i$ we have that

$$lkq'_i + lr'_i \equiv kq_i + r_i \pmod{kn}.$$

Then, there are some integers e and f such that $r_i = lr'_i - ek$ and $q_i = lq'_i + e - fn$. Hence,

$$a_i = q_i + nr_i = (lq'_i + e - fn) + n(lr'_i - ek) = l(q'_i + nr'_i) + e - fn - enk.$$

This implies that a_i is obtained from b_i by multiplying l and adding $e - fn - enk$. Since l is relatively prime to kn , (n, k) -sequence $\{a_i\}$ is obtained from (n, k) -sequence $\{b_i\}$ by transformations (A), (M), and (P). Thus two (n, k) -sequences $\{a_i\}$ and $\{b_i\}$ are “essentially the same”. \square

Example 3. For the prime $p = 13$ one can construct (n, k) -sequences of the parameters $(12, 1)$, $(6, 2)$, $(4, 3)$, $(3, 4)$, $(2, 6)$, and $(1, 12)$ using primitive roots 2, 2^5 , 2^7 , and 2^{11} . Fig. 3 shows that $(4, 3)$ and $(3, 4)$ -sequences using primitive roots 2 and 2^5 . Consider the $(4, 3)$ -sequence using a primitive root 2^5 . Take a partition with $S_0 = \{0, 3, 1, 2\}$, $S_1 = \{7, 4, 6, 5\}$, and $S_2 = \{9, 10, 8, 11\}$ and multiply this sequence by 5 modulo 4 and add 0 modulo 4 in S_0 , 1 modulo 4 in S_1 , and 3 modulo 4 in S_2 and then using transformation (P) we replace $a_i \in S_1$ by $b_i \in S_2$ and $a_i \in S_2$ by $b_i \in S_1$ so that we can obtain an $(4, 3)$ -sequence $\{b_i\} = \{0, 4, 5, 8, 3, 9, 11, 1, 10, 7, 6, 2\}$ which is already obtained by using a primitive root 2.

3. Other properties of (n, k) -sequences

Now, we study some properties of the (n, k) -sequences determined by the construction in Theorem 2.

For $l = 1, 2, \dots, n-1$ let N_l be the number of l 's in the difference \pmod{n} triangle of an (n, k) -sequence $\{a_i\}$, and let $N = \sum_{l=1}^{n-1} N_l$. For each $j = 0, 1, \dots, k-1$ let S_j be the j th comparable part of $\{a_i \mid 1 \leq i \leq nk\}$ i.e., $S_j = \{a_i \mid a_i = nj + t; t = 0, 1, \dots, n-1\}$. Then, for each $l = 1, 2, \dots, n-1$, since S_j contains every residue mod n exactly once,

$(n, k) = (4, 3)$ $g = 2$	r_i	0	1	1	2	0	2	2	0	2	1	1	0
	q_i	0	0	1	0	3	1	3	1	2	3	2	2
	$a_i = q_i + 4r_i$	0	4	5	8	3	9	11	1	10	7	6	2
$(n, k) = (4, 3)$ $g = 2^5$	r_i	0	2	2	1	0	1	1	0	1	2	2	0
	q_i	0	1	2	3	3	0	2	1	1	0	3	2
	$a_i = q_i + 4r_i$	0	9	10	7	3	4	6	1	5	8	11	2
$(n, k) = (3, 4)$ $g = 2$	r_i	0	1	0	2	1	1	3	3	0	2	3	2
	q_i	0	0	1	0	2	1	2	0	2	2	1	1
	$a_i = q_i + 4r_i$	0	3	1	6	5	4	11	9	2	8	10	7
$(n, k) = (3, 4)$ $g = 2^5$	r_i	0	1	0	2	1	1	3	3	0	2	3	2
	q_i	0	1	2	2	2	0	1	0	1	0	2	1
	$a_i = q_i + 4r_i$	0	4	2	8	5	3	10	9	1	6	11	7

Fig. 3. Examples of (n, k) -sequences for $p = 13$.

the residue $t + 1$ occurs either to the right of t or to the left of t (not both) exactly once for all $t = 0, 1, \dots, n - 1$. This shows that for each $l = 1, 2, \dots, n - 1$

$$N_l + N_{n-l} = kn \quad \text{and hence} \quad N = kn(n - 1)/2.$$

Note that the sequence $\{a_i\}$ does not have to be an (n, k) -sequence in order to obtain the above result. That is, it is sufficient that $\{a_i\}$ is a permutation of $0, 1, 2, \dots, nk - 1$.

Theorem 4. Let $p = nk + 1$ be a prime, and $\{a_i\}$ be an (n, k) -sequence determined by the construction in Theorem 2. In the difference (mod n) triangle we have $N_l = kn/2$ for $l = 1, 2, \dots, n - 1$. Further, if n is even then the middle column in the difference (mod n) triangle contains $n/2$ exactly $nk/2$ times and if n is odd then the middle column in the difference (mod n) triangle does not contain any number.

Proof. For each i and d with $1 \leq i < i + d \leq kn$, let $i = g^j$, $i + d = g^{j_1}$, $p - i = g^{j'}$ and $p - (i + d) = g^{j'_1}$ where g is a primitive root modulo p and $0 \leq j, j_1, j', j'_1 \leq nk - 1$. From $i = g^j$ and $p - i = g^{j'}$ we have that

$$g^{j'} = p - i = -g^j = g^{(p-1)/2} g^j = g^{(p-1)/2+j} = g^{nk/2+j}$$

and hence

$$\frac{nk}{2} + j \equiv j' \pmod{nk}. \quad (1)$$

Similarly, $g^{j'_1} = p - (i + d) = g^{nk/2+j_1}$ implies that

$$\frac{nk}{2} + j_1 \equiv j'_1 \pmod{nk}. \quad (2)$$

Hence, a_i and a_{i+d} are comparable if and only if $j \equiv j_1 \pmod{k}$ iff $j' \equiv j'_1 \pmod{k}$ iff a_{p-i} and a_{p-i-d} are comparable. Thus, if (a_i, a_{i+d}) is a comparable pair then we have

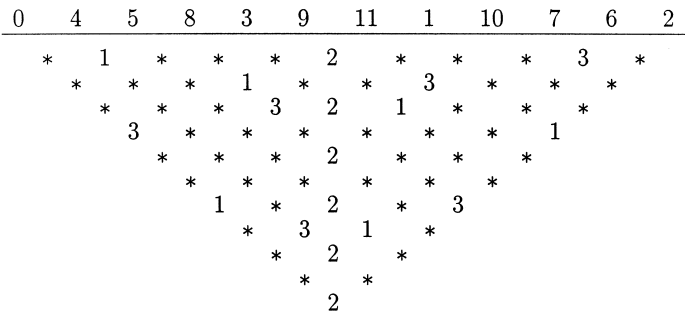


Fig. 4. Difference triangle of (4,3)-sequence.

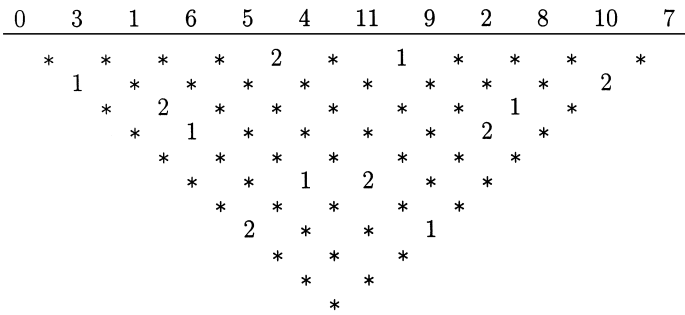


Fig. 5. Difference triangle of (3,4)-sequence.

that

$$a_{i+d} - a_i \equiv \frac{1}{k} \text{Ind}_g \frac{i+d}{i} \pmod{n},$$
$$a_{p-i} - a_{p-i-d} \equiv \frac{1}{k} \text{Ind}_g \frac{p-i}{p-i-d} \equiv \frac{1}{k} \text{Ind}_g \frac{i}{i+d} \pmod{n}.$$

Therefore, $(a_{i+d} - a_i) + (a_{p-i} - a_{p-i-d}) = n$. Since $N_l + N_{n-l} = kn$, we have that $N_l = N_{n-l} = kn/2$ for $l = 1, 2, \dots, n - 1$. Now if n is even then from (1) we have that $j \equiv j' \pmod{k}$ and thus a_i and a_{p-i} are comparable for all $i = 1, 2, \dots, nk$. Thus, the middle column in the difference \pmod{n} triangle contains the number

$$a_{p-i} - a_i = \frac{1}{k} \text{Ind}_g(-1) = \frac{n}{2}.$$

exactly $nk/2$ times. On the other hand, if n is odd then (1) shows that a_i and a_{p-i} are not comparable for all $i = 1, 2, \dots, nk$. Thus, the middle column in the difference \pmod{n} triangle does not contain any number. \square

We have (4,3), and (3,4)-sequences in Fig. 3. Using these two sequences we obtain the difference triangles of (4,3)-, and (3,4)-sequences (Figs. 4–6) which explain the results in Theorem 4.

0	6	1	11	10	8	4	5	2	7	9	3
*	*	*	5	4	*	1	3	*	2	*	
	1	5	*	3	*	*	4	*	*	*	
		*	4	*	*	*	*	*	*	1	
			*	2	3	*	5	*	4		
				*	4	*	1	5	*		
				4	*	1	2	*			
					5	*	4	*			
					2	1	*	*			
						*	3	2			
							*	*			
								3			

Fig. 6. Difference triangle of (6,2)-sequence.

However, Theorem 4 does not hold for some (n, k) -sequences which are not constructed by using a primitive root modulo p . For instance, a (6, 2)-sequence in Fig. 6 shows that $N_1 = 6$, $N_2 = 5$, $N_3 = 6$, $N_4 = 7$, and $N_5 = 6$.

Given an (n, k) -sequence $\{a_i\}$ of length nk , let $\{c_i\}$ be the k -ary sequence of length nk determined by the rule $c_i = j$ for some $j = 0, 1, \dots, k - 1$ if $a_i \in S_j$ where S_j is the j th comparable part of the (n, k) -sequence $\{a_i\}$. In this k -ary sequence t consecutive i 's surrounded by symbols other than i on the left and right is called a “run” of length t . Now, (a_i, a_j) is a comparable pair if and only if $c_i = c_j$, and in this case we also call (c_i, c_j) comparable. In this sequence of c_j 's, let R be the total number of runs, R_i the number of runs of length i , and C_i the number of comparable pairs of the form (c_s, c_{s+i}) .

Theorem 5. Let $\{a_i\}$ be an (n, k) -sequence and $\{c_i\}$ be the corresponding k -ary sequence. Then, in the sequence of c_i 's, the total number R of runs is at least $n(k - 1) + 1$ and at most $((k + 1)/2)n + ((R_1 - 1)/2)$. Further, we have $((k - 1)/2)n - ((R_1 - 1)/2) \leq C_1 \leq n - 1$ and $n(k - 1) + 1 - (R_1 + R_2) \leq C_2 \leq n - 1$.

Proof. Since there are R runs in the sequence $\{c_i\}$ if and only if there are $R - 1$ incomparable adjacent pairs, we have that $C_1 = (nk - 1) - (R - 1) = nk - R$. But obviously $C_1 \leq n - 1$ and hence $R \geq n(k - 1) + 1$. To obtain the upper bound on R we compute the following:

$$nk - R = \sum_{i \geq 1} iR_i - \sum_{i \geq 1} R_i = \sum_{i \geq 2} (i - 1)R_i \geq R_2$$

and hence we obtain $R \leq nk - R_2$, also from the following inequality:

$$\begin{aligned} n - 1 &\geq C_2 \geq \sum_{i \geq 3} (i - 2)R_i \\ &= R + \sum_{i \geq 4} (i - 3)R_i - (R_1 + R_2) \\ &\geq R - (R_1 + R_2), \end{aligned}$$

we obtain that $R \leq (n-1) + R_1 + R_2$. Thus, we have that $R \leq ((k+1)/2)n + ((R_1-1)/2)$. Further, $((k-1)/2)n - ((R_1-1)/2) \leq C_1 \leq n-1$ since $C_1 = nk - R$ and we have that

$$n-1 \geq C_2 \geq R - (R_1 + R_2) \geq n(k-1) + 1 - (R_1 + R_2).$$

Thus, the proof is completed. \square

Theorem 6. Let $p = nk + 1$ be an odd prime, $\{a_i\}$ be an (n, k) -sequence constructed using a primitive root modulo p , and $\{c_i\}$ be the corresponding k -ary sequence. Then we have that

- (1) $C_i \leq n-1$ for $i = 1, 2, \dots, p-2$.
- (2) $C_1 = n-1$ and hence $R = n(k-1) + 1$.
- (3) $C_2 = n-1$ if n is odd and $C_2 = n-2$ if n is even.

Proof. Statement (1) is obvious. For (2) and (3), we proceed as follows. An (n, k) -sequence $\{a_i\}$ can be partitioned into comparable parts

$$S_j = \{jn, jn+1, jn+2, \dots, jn+(n-1)\} \quad \text{for } j = 0, 1, \dots, k-1.$$

Let g be a primitive root modulo p . If $\{a_i\}$ is constructed from g as in Theorem 2, then we have $a_i = q_i + nr_i \in S_j$ iff $j = r_i$ and $(q_i, r_i) \in \{(0, j), (1, j), \dots, (n-1, j)\}$ iff $\text{Ind}_g(i) \in \{j, k+j, 2k+j, \dots, (n-1)k+j\}$ iff $i \in \{g^j, g^{k+j}, \dots, g^{(n-1)k+j}\}$. Therefore, the partition S_0, S_1, \dots, S_{k-1} of $\{0, 1, 2, \dots, kn-1\}$ induces a partition E_0, E_1, \dots, E_{k-1} of $\{1, 2, \dots, kn\}$ as follows: $a_i \in S_j$ iff $i \in E_j = \{g^j, g^{k+j}, \dots, g^{(n-1)k+j}\}$.

Now, since a_i and a_{i+d} are comparable iff both a_i and a_{i+d} belong to S_j for some j iff both i and $i+d$ belong to E_j for some j , we need to compute the number of disjoint pairs (m, t) satisfying $g^t - g^{t+mk} = \pm 1$ where $0 \leq t \leq nk-1$, $1 \leq m \leq n-1$. Obviously, for each m ($1 \leq m \leq n-1$), there exists unique integer t ($0 \leq t \leq nk-1$) for which $g^t(1 - g^{mk}) = 1$. However, we have that

$$g^t(1 - g^{mk}) = 1 = g^{nk/2+t+mk}(1 - g^{(n-m)k}).$$

Thus we have at most $\lfloor n/2 \rfloor$ solutions for which $g^t(1 - g^{mk}) = 1$. Similarly, we have at most $\lfloor n/2 \rfloor$ solutions for which $g^t(1 - g^{mk}) = -1$. If n is even, then $g^t(1 - g^{nk/2}) = 1$ implies that $g^{t+nk/2}(1 - g^{nk/2}) = -1$. Therefore, we have at most $n-1$ solutions (m, t) to $g^t(1 - g^{mk}) = \pm 1$ with $1 \leq m \leq \lfloor n/2 \rfloor$. It is easy to check that each one of $n-1$ solutions (m, t) contributes to a comparable pair of length 1. Thus, $C_1 = n-1$ and hence $R = n(k-1) + 1$. This proves (2). Similarly, we have $n-1$ solutions to $g^t(1 - g^{mk}) = \pm 2$. However, in this case we counted the pair (a_1, a_{nk}) since $nk-1 = -2 \pmod{p}$. Of course, it is not a pair of length 2. But, we know that (a_1, a_{nk}) is a comparable pair if and only if n is even. Thus we have proved (3). \square

4. Number of $(n, 2)$ -sequences

Finally, we present an updated table of essentially distinct $(n, 2)$ -sequences for n up to 13 in Table 1. The number $w_2(n)$ is the number of essentially distinct $(n, 2)$ -sequences

Table 1
The number $w_2(n)$ of essentially distinct $(n, 2)$ -sequences

n	$2n$	$w_2(n)$	CPU time	$(n, 2)$ -sequences $\{a_i\}$
1	2	1		01 ^a
2	4	1		0231 ^a
3	6	2		<u>013254^a</u> 035124
4	8	2 ^b		<u>01465372</u> 04217563
5	10	5		<u>0159738246</u> 0513476928 <u>0514367928^a</u> 0589173246 0596184237
6	12	4	~ 0.0 s	<u>026B831A4957</u> 06218A7B4593 <u>0621A8B74593^a</u> 061BA8452793
7	14	8	~ 2.0 s	017B24D5CA3698 <u>017B64C3D825A9</u> <u>07148AB6539D2C</u> <u>071CA524D986B3</u> <u>07A124958DC63B</u> <u>07B1395A48D62C</u> <u>0791AB8365D42C</u> 079A14D28C653B
8	16	6 ^b	~ 1.6 min	0182AFD379BE6C54 <u>0182E9B37FDA6C54^a</u> 018AD3B26F79EC54 <u>018EB3D2697FAC54</u> 089F27E51A36BDC4 089F61E37A52BDC4
9	18	1	~ 5 min	$2n + 1 = 19$ is prime
10	20	0	~ 140 min	NONE
11	22	1 ^b	~ 7 h	$2n + 1 = 23$ is prime
12	24	0 ^b	~ 14 days	NONE
13	26	0 ^b	~ 130 days	NONE
14	28	≥ 1	?	$2n + 1 = 29$ is prime
15	30	≥ 1	?	$2n + 1 = 31$ is prime
16	32	?	?	?

^aIndicates that it is from the prime construction in Theorem 2.
^bTwo corrections, $w_2(4)$ and $w_2(8)$, three more terms based on some extensive computations.

[10] and appears also in [7] with ID number A007281 for n up to 10. Table 1 shows two corrections, $w_2(4)$ and $w_2(8)$, and three more terms based on some extensive computations. These are represented by footnote b. The horizontal lines between the sequences inside the same n signifies distinct binary sequences induced from $\{a_i\}$.

The footnote a indicates that it is from the prime construction in Theorem 2. For $n \geq 10$, the symbol A, B, C, ... are used to denote 10, 11, 12, ..., etc. CPU time is based on DEC-Alpha PC with 533 MHz clock speed. The smallest n for which the existence is open now becomes 16, and the smallest n for which the exact value of $w_2(n)$ is not yet determined becomes 14.

References

- [1] T. Etzion, S.W. Golomb, H. Taylor, Tuscan- k squares, *Adv. Appl. Math.* 10 (1989) 164–174.
- [2] S.W. Golomb, T. Etzion, H. Taylor, Polygonal path constructions for Tuscan- k squares, *Ars Combin.* 30 (1990) 97–140.
- [3] S.W. Golomb, H. Taylor, Two-dimensional synchronization patterns for minimum ambiguity, *IEEE Trans. Inform. Theory* IT-28 (1982) 600–604.
- [4] S.W. Golomb, H. Taylor, Tuscan squares – A new family of combinatorial designs, *Ars Combin.* 20-B (1985) 115–132.
- [5] A. Lempel, H. Greenberger, Families of sequences with optimal Hamming correlation properties, *IEEE Trans. Inform. Theory* IT-20 (1974) 90–94.
- [6] A.A. Sharr, P.A. Davies, Prime sequences: quasi-optimal sequences for OR channel code division multiplexing, *Electron. Lett.* 19 (1983) 888–890.
- [7] N.J.A. Sloane, S. Plouffe, *The Encyclopedia of Integer Sequences*, Academic Press, San Diego, 1995, On-line version in: <http://www.research.att.com/~njas/sequences>.
- [8] H.Y. Song, On aspects of Tuscan squares, Ph.D. Thesis, University of Southern California, 1991.
- [9] H.Y. Song, On the existence of circular Florentine arrays, *Comput. Math.*, to appear.
- [10] H.Y. Song, S.W. Golomb, Generalized Welch–Costas sequences and their application to Vatican arrays, in: G.L. Mullen, P.J. Shiue (Eds.), *Finite Fields: Theory, Applications, and Algorithms*, American Mathematical Society, Providence, RI, 1994, pp. 341–351.
- [11] H.-Y. Song, J.H. Dinitz, Tuscan squares, in: C.J. Colbourn, J.H. Dinitz (Eds.), *CRC Handbook of Combinatorial Designs*, CRC Press, New York, 1996, pp. 480–484.
- [12] H.Y. Song, I. Reed, S.W. Golomb, On the non-periodic cyclic equivalence classes of RS codes, *IEEE Trans. Inform. Theory* IT-39 (1993) 1431–1434.
- [13] H. Taylor, Florentine rows or left-right shifted permutation matrices with cross-correlation values ≤ 1 , *Discrete Math.* 93 (1991) 247–260.
- [14] T.W. Tilson, A Hamiltonian decomposition of K_{2m}^* , $2m \geq 8$, *J. Combin. Theory* B-29 (1980) 68–74.